Pregunta **1**

Enunciado de la pregunta

a) Menciona y describe brevemente con tus palabras un esquema criptográfico asimétrico basado en el problema de la mochila que hayamos visto en clase.

b) La propiedad de seguridad llamada "binding" , ¿en qué tipo de esquemas es relevante? Explica con un ejemplo inspirado en una aplicación práctica por qué es importante.

Pregunta **2**

Enunciado de la pregunta

NOTACIÓN "b^c" representa "b elevado a c"

Supongamos que en la generación de claves del cifrado de Bellare y Rogaway la función f de involucrada es una función exponenciación, es decir, coge un elemento x de un conjunto X y hace f(x) = x^a para un cierto número a secreto y fijado.

Escribe,

a) como se realiza el cifrado y el descifrado de mensajes en este caso concreto.

b) las hipótesis que son necesarias para que el esquema resultante sea seguro en el sentido que se persigue en la construcción genérica de Bellare y Rogaway.

Pregunta **3**

Enunciado de la pregunta

Supongamos que un esquema de cifrado es NM-CPA.

¿Podría ocurrir que un adversario CCA capturase un texto cifrado c de un texto m en el canal, lo modificase, y construyese así un cifrado c2 válido que el receptor descifrara como 2m?

Pregunta **4**

Finalizado

Enunciado de la pregunta

notación: "a_b" se lee "a sub b", es decir, indica que b es un subíndice de a

Supongamos que implementamos un esquema de Shamir sobre

Z_7 ={0,1,2,3,4,5,6}

para repartir el secreto "2" entre 5 participantes, de modo que el umbral de reconstrucción sea 3.

Haz una generación de las "shares" o "fragmentos" para los 5 participantes. Explica por qué si se juntan solo 2 no podrán recuperar el secreto.

Pregunta **5**

Enunciado de la pregunta

Notación: "a^b" quiere decir "a elevado a b"

El departamento de TICs de la empresa CRYPTOGUAY genera claves RSA para que todos los empleados puedan comunicarse con seguridad. La clave pública de la ingeniera Alicia es (N=49163,e= 1 + 2^16).

Eva es un adversario que sólo dispone de una pieza de hardware que recibe tres números de entrada, a,b y M y da como salida a^b mod M. Eva, la pobre, no puede hacer ninguna otra operación.

Describe un método pienses que puede servirle a Eva para encontrar la clave secreta de Alicia.